

网络基础设施维保服务项目

# 竞争性谈判文件

采 购 人：青岛交通科技信息有限公司

项目编号：QDJTKJCG-20230020

日 期：2023 年 12 月 21 日

## 第一章 竞争性谈判公告

青岛交通科技信息有限公司对网络基础设施维保服务项目以竞争性谈判方式组织采购，欢迎符合条件的供应商参加报价。

### 一、项目基本情况：

项目编号：QDJTKJCG-20230020

项目名称：网络基础设施维保服务项目

采购方式：竞争性谈判

预算金额：标包【1】：35万元；

最高限价：标包【1】：35万元；

需求公示时间：该项目采购需求公示期3日。

项目联系方式：采购单位：青岛交通科技信息有限公司

地址：青岛市李沧区北园路三号

联系方式：0532-88969795

### 二、供应商的资格要求：

2.1 具有独立承担民事责任能力的法人，提供营业执照副本复印件且加盖公章。

2.2 通过“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）查询，未被列入失信被执行人、重大税收违法案件当事人、政府采购严重违法失信行为记录等名单的，提供查询页面复印件且加盖供应商公章。

### 三、开标时间：

3.1 时间：2023年12月28日14:30时

3.2 地点：青岛市李沧区北园路3号二楼会议室

## 第二章 供应商须知前附表

序号	条款名称	编列内容
1	采购人	青岛交通科技信息有限公司
2	项目名称	网络基础设施维保服务项目
3	分包情况	不分包
4	资金来源以及资金构成	自筹资金
5	是否接受联合体报价	<input checked="" type="checkbox"/> 不接受 <input type="checkbox"/> 接受

6	报价有效期	自报价截止之日起 <u>30</u> 个日历天。
7	是否开展需求调查	否。
8	履约担保	<input checked="" type="checkbox"/> 不需要 <input type="checkbox"/> 需要，履约保证金的金额：成交合同金额的%（履约保证金须以支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式提交）
9	报价截止时间	详见磋商谈判文件“第一章 竞争性谈判公告”
10	是否允许递交备选报价方案	<input checked="" type="checkbox"/> 不允许 <input type="checkbox"/> 允许。要求：只有成交供应商所递交的备选报价方案方可予以考虑。磋商小组认为成交供应商的备选报价方案优于其按照谈判文件要求的报价方案，采购人可以接受该备选报价方案。
11	响应报价的范围	含税全包价。包含提供相关服务的所有费用，合同存续期间采购人不额外支付任何费用。
12	响应文件编制装订	1. 响应文件的商务部分和技术部分左侧胶装成册（建议合并胶装为一册，若页数较多可分册）。 2. 封面设置。响应文件封面设置包括：响应文件、项目名称、项目编号、供应商全称和响应文件完成时间。供应商全称填写“×××公司”。 3. 响应文件内容。供应商应按照谈判文件的要求编写响应文件。 4. 响应文件正文用白色 A4 复印纸双面打印，建议编制目录及标注连续页码，左、下侧对齐。
13	响应文件签署和盖章	1. 谈判文件要求供应商法定代表人或者被授权代表签字处，均须签字并加盖单位公章。 2. 被授权代表人签字的，响应文件应附法人授权委托书。 3. “报价函”、“法人授权委托书”和“政府采购诚信承诺书”必须由法定代表人签字或盖章。 4. 供应商在响应文件以及相关书面文件中的单位盖章（包括印章、公章等）均指与供应商名称全称相一致的标准公章，不得使用其他形式（如带有“专用章”、“合同章”、“财务章”、“业务章”等）的印章。
14	响应文件份数及要求	响应文件应按包分别进行编制： 1. 响应文件正本 <u>壹</u> 份，副本 <u>贰</u> 份。正本和副本

		<p>的封面上应当清楚地标记“正本”或者“副本”字样；正本和副本不一致时，以正本为准。</p> <p>2. 资格、资信等证明文件；</p> <p>3. 电子版响应文件壹套：内容与纸质响应文件正本一致，格式：PDF 格式；介质：“U”盘或者光盘。</p>
15	响应文件密封和标记	<p>1. 分为二个密封件，分别是：<u>响应文件密封件；资格、资信等证明文件密封件（详见第三章内容，包括电子版响应文件）。</u></p> <p>注：一个密封件确实无法密封的，可分开密封；对于投多个包的供应商，资格、资信等证明文件可密封为一个密封件。</p> <p>2. 密封件封套上标明采购项目编号、项目名称以及包、供应商名称等，在所有封签处标注“请勿在年月日时分之前启封”字样，并加盖供应商单位公章以及法定代表人或者被授权代表签字。</p> <p>3. 法定代表人授权委托书原件和本人身份证原件应当在递交响应文件时出示并提交，不允许放在密封件中。</p>
16	递交响应文要求	<p>供应商应当在谈判文件要求提交响应文件的截止时间前，将响应文件密封送达开标地点。</p> <p>递交响应文件时：被授权代表应出示授权委托书原件和本人身份证原件以证明其出席。</p> <p>否则，对递交的响应文件将不予接收。</p>
17	开标时间及地点	详见磋商谈判文件“第一章 竞争性谈判公告”

### 第三章 供应商应当提交的资格、资信等证明文件

#### 1. 资格、资信等证明文件目录

序号	证明材料名称	提供形式	备注
1	具有独立承担民事责任能力的企业或组织合法经营权的凭证（如营业执照、登记证书、执业许可证等）	<input checked="" type="checkbox"/> 复印件	
2	法定代表人身份证明和本人身份证或法定代表人授权委托书和本人身份证	原件	
3	“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网(www.ccgp.gov.cn)网站查询截图。	<input checked="" type="checkbox"/> 网站查询截图	
4	招标公告发布之日前三年内在经营活动中无行贿犯罪等重大违法记录	<input checked="" type="checkbox"/> 网站查询截图	
5	评分办法中所需的其他证明材料		

备注：

(1) 开标时，供应商应当提交上述证明材料，未提交或提交不全的视为资格性、符合性审查不合格；

(2) 要求提供的证明材料可以是复印件的，需加盖供应商公章。

(3) 供应商的资格证明材料应当真实、有效、完整，字迹、印章要清晰。

## 第四章 采购需求

### 1. 采购标的汇总表

包号	序号	标的名称	计量单位	数量
1	1	网络基础设施维保服务项目	宗	1

### 2. 技术要求：

#### 1. 项目说明

1.1 本章内容是根据采购项目的实际需求制定的。

1.2 本项目共分为 1 个包进行招标。供应商所报价格应为含税全包价，包含提供相关服务的所有费用，合同存续期间采购人不额外支付任何费用。

#### 2. 采购要求

##### 2.1 项目概况

网络及安全基础维保服务主要承担边界防火墙、路由器、交换机运维、策略优化等，承担网络安全设备维保服务和部分重点设备特征库升级。

##### 2.2 总体要求

服务供应商应符合国家法律法规及相关技术要求，企业各项管理规章制度完善，具备相应规模项目运维服务经验，制定详细的运维服务方案，能充足配备符合项目要求的运维服务岗位人员，按要求按时保质保量完成项目工作，按照采购方要求完成其他有关工作。

1. 安全责任事故零发生；

2. 各项运维服务协助工作响应率 100%;

3. 各项运维服务管理制度完善完备;

4. 服务考核月平均合格率  $\geq 95\%$ ;

5. 有理投诉为零;

6. 服从采购人管理, 以确保采购人履职为原则, 完成双方合同约定外难以提前预估的合理工作任务。

### 2.3 基本需求

1. 供应商须接受采购人的监督和管理, 严格按合同和采购人现有管理办法等要求提供运维服务。

2. 供应商要建立健全各种规章制度, 符合国家法律法规、符合项目技术要求。

3. 供应商要具备相应规模项目 2 年以上的运维服务经验, 并证明相关业务业绩。

4. 供应商在签订合同后 15 个工作日内, 要结合本项目实际编制详尽的服务方案, 方案中应包括不限于服务内容、驻场运维人员名单、人员基本情况、工作职责、考核办法及其他事项。

### 2.4 服务要求

#### 2.4.1 基本内容运维事项

服务主要涉及安全设备特征库升级服务、安全设备运维服务、网络交换设备运维服务工作, 具体内容如下:

##### (1) 安全设备特征库升级服务

①EDR 特征库在保, 维持 300 点服务器端授权、450 点 PC 端授权;

②深信服设备特征库更新；

③防火墙威胁防护特征库升级(URL 库、IPS 漏洞特征防护库、应用识别库、WEB 应用防护库、数据泄密防护库、实时漏洞分析识别库、僵尸网络与病毒防护库、热点事件库)；

④数据中心 WAF 防护特征库升级更新；

⑤数据中心 IPS 特征库升级更新；

⑥防火墙、IPS、WAF、VPN、网闸等设备版本升级更新；

⑦开展其他安全系统常规运维工作（如 TSOC-USM 泰合信息安全运营中心系统）。

## (2) 安全设备运维服务

①VPN 设备、负载均衡设备、网闸设备无需原厂维护，开展常规运维工作；

②近海和危化品项目漏洞扫描 1 台、态势感知 1 台、日志审计 1 台、数据库审计 1 台、堡垒机 1 台、互联网防火墙 1 台、入侵检测 1 台、负载均衡 2 台、分支防火墙 20 台等设备维保，开展常规运维工作；

③强化安全特征库管理，确保互联网安全设备特征库实时更新，定期更新设备安全特征库。

## (3) 网络交换设备运维服务

对交通运输专网相关设施（包括外联单位）进行日常巡检和故障排查，保络设备正常运行，确保网络不中断。通过分析网络配置，提供优化方案并解决存在的安全风险和隐患。

★因设备性能不足不能满足系统运转需要，或者因设备故障维修成本过高，应采购人要求，成交供应商应配合完成相应设备更替。

运维设备清单如下表：

序号	设备名称	主要性能、功能	单位	数量
(一) 路由器设备				
1.	专用一体化路由器	8 口千兆 POE 多功能网关路由器 10 个 10/100/1000M 电口，其中最多支持 4 个 WAN 口(默认 2 个 WAN 口，8 个 LAN 口；其	台	1



序号	设备名称	主要性能、功能	单位	数量
		中 LAN6/L AN7 可以切换为 WAN 口)		
2.	交通运输专用交换机 48 口	48 口 10/100/1000M 自适应电口, 4 个 SFP+万兆光口, 固化交流电源	台	2
3.	交通运输专用 POE 交换机 24 口	固化 24 个 10/100/1000M 自适应电口, 4 个 1GSFP 光口, 1-24 口支持 PoE+/PoE, 1-4 号口支持 HPoE (60W), 整机 PoE 最大输出 370W。	台	2
4.	专用无线控制器	多业务无线控制器, 自带 8 个千兆电口, 1 个; SFP 口, 1 个 SFP+口; 可通过扩展 License 最大控制 800 个 AP; 标配一个电源 (含扩展授权)。扩展授权: 系列无线控制器产品专用升级许可证 License, 每套可支持增加 16 个普通 AP 或 32 个墙面式 AP 的控制权, 本次结合设备默认支持 AP 数量配置, 保障整机实际配置支持 128 个 AP	台	1
5.	专用双频千兆无线路由器	网络标准 IEEE 802.11a/b/g/n/ac/ax 无线协议; 最高传输速率 5952Mbps; 传输速率 2.4GHz 频段: 1148Mbps; 5GHz 频段: 4804Mbps 频率范围 双频(2.4GHz, 5GHz); 网络接口 4 个 10/100/1000Mbps 速率自适应以太网接口, 支持 WAN/LAN 自适应(网口盲插)	台	1
6.	专用双频千兆无线路由器	网络标准 IEEE 802.11a/b/g/n/ac/ax 无线协议; 最高传输速率 5952Mbps; 传输速率 2.4GHz 频段: 1148Mbps 5GHz 频段: 4804Mbps 频率范围 双频(2.4GHz, 5GHz); 网络接口 4 个 10/100/1000Mbps 速率自适应; 以太网接口, 支持 WAN/LAN 自适应(网口盲插)	台	1
7.	交通运输专用交换机	交换容量: 336Gbps 包转发率: 51Mpps 固定端口:24 个 10/100/1000Base-T 以太网端口, 4 个千兆 SFP, POE 总功率为 380W	台	1
8.	交通运输专用交换机	交换容量: 672Gbps 包转发率: 252Mpps 固定端口:48 个 10/100/1000Base-T 以太网端口, 4 个万兆 SFP+, POE 总功率为 1440W, 支持 1+1 电源备份	台	1

序号	设备名称	主要性能、功能	单位	数量
9.	运维管理系统	提供丰富的资源管理视图，对不同品牌、类型、版本的网络设备、安全设备、无线设备、服务器、中间件、数据库等 IT 资源进行统一、全方位、多层次的综合管理，提供设备分组管理，设备访问模板管理，接口组管理，网络用户组，推送页面配置，特征库，软件版本，配置管理，设备告警，设备系统日志，设备操作日志，WEB 网站防护等统一管理，实时掌握资源的运行状态和性能变化	台	1
10.	局机关无线控制器	业务端口 4 个千兆光口、4 个千兆电口；2 个万兆光口扩展插槽，提供双电源冗余；基础可管理 AP 数目 64 个；最大可管理 AP 数目 512 个，可增加不同的 License 灵活扩展。	台	2
11.	局机关无线 AP	射频设计：双路双频设计，支持 3 条空间流传输协议；可支持 802.11a/b/g/n 和 802.11ac 同时工作天线类型：内置 X-sense 灵动天线阵列，且数量高达 24 根	台	32
12.	局机关 POE 交换机	24 口 10/100/1000M 自适应电口交换机（支持 30W 的 PoE+远程供电），8 个复用的 SFP 接口，2 个扩展槽，2 个模块化电源插槽，RG-M5000E-AC500P 电源模块	台	3
13.	千兆接入交换机（万兆上联）	设备指标：千兆电口 44 个，千兆光电复用口 4 个，配置 1 端口万兆光口扩展卡 1 块，性能指标：交换容量 320Gbps，整机转发性能 132Mpps	台	6
14.	管理网络交换机	交换容量 256Gbps，转发性能 96Mpps，千兆电口 24 个，配置非复用 4 端口千兆光扩展卡一块；支持流镜像，支持端口镜像，支持基于端口的 VLAN，支持基于 MAC 的 VLAN，支持基于认证策略的 VLAN	台	2
15.	终端接入交换机 1	交换容量 $\geq 256$ Gbps，转发性能 $\geq 131$ Mpps；千兆电口 $\geq 48$ ，千兆光口 $\geq 4$ （非复用接口），并配置 2 个千兆多模模块；	台	4
16.	终端接入交换机 2	交换容量 $\geq 256$ Gbps，转发性能 $\geq 131$ Mpps；千兆电口 $\geq 24$ ，千兆光口 $\geq 4$ （非复用接口），并配置 2 个千兆多模模块	台	4
17.	专网核心交换机 3	CLOS 多级多平面交换架构，系统交换容量：102.4Tbps，包转发能力：24000Mpps。配置主控引擎 2；独立交换网板 2；整机业务板槽位数 4，支持模块化风扇框，可热插拔，独立风扇框数 2；配置双主控引擎，冗余交流电源；配置独立交换网板；配置 16 个万兆光口用于集群，配置相关线缆模块，配置 48 千兆	台	2

序号	设备名称	主要性能、功能	单位	数量
		电口。		
18.	接入交换机 3	集成无线控制器功能；交换容量:580G；包转发率:168Mpps；支持 28 个千兆电口，4 个复用千兆光 Combo 口，4 个千兆光口。	台	2
19.	专用无线 AP	1 个 2.5G 以太网口，1 个 10/100/1000Mbps 自适应以太网口，最大用户数不少于 256 个，室内放装型无线接入点，三路双频，支持 6 条空间流，整机最大接入速率 3.267Gbps，双网口设计，支持标准的 802.11ax 协议，可同时工作在 802.11ax 和 802.11a/b/g/n/ac 模式，胖/瘦模式切换	台	11
(二) 交通专网外联路由器				
1.	分支机构路由器	MSR5620，转发性能 $\geq 16$ Mpps，配置 2 个万兆光口，6 个千兆光口，5 个千兆电口，所有端口均非复用接口，并配置 2 个千兆单模模块；整机可扩展业务插槽数 $\geq 6$ ，USB 接口数 $\geq 2$ ；支持冗余主控，支持冗余电源。	台	4
2.	边界路由器	RG-RSR30-X，固化 9 个 GE 接口，其中 8Combo，内存 2G，支持静态路由、RIPv1/v2、OSPFv2、BGP、IS-IS、策略路由、路由策略等	台	18
(三) 安全防护设备				
1.	互联网接入防火墙	吞吐量：10 Gbps；并发连接数：2,600,000；每秒新建连接数：500,000；标配网口：6 个千兆电口，2 个千兆光口；1 个扩展槽；硬件 BYPASS，支持；硬盘：500GB	台	2
2.	入侵防御设备	吞吐量：8 Gbps，并发连接数 2,200,000，每秒新建连接数：450,000，标配网口：8 个千兆电口，2 个千兆光口，1 个扩展槽，硬件 BYPASS：支持，硬盘：500GB.	台	2
3.	负载均衡设备	设备指标：分布式多核硬件架构，非 X86 工控机架构，千兆独立电口 6 个，千兆独立光口 2 个，扩展槽位 1 个，配置双交流电源	台	1

序号	设备名称	主要性能、功能	单位	数量
4.	负载均衡设备	配置双交流电源；4个千兆电端口，4个千兆光端口（配置2个多模光模块）；设备吞吐量4Gbps，最大并发连接数400万，四层每秒新建连接数18万，七层每秒新建连接数36万。单一设备可同时支持包括链路负载均衡、全局负载均衡和服务器负载均衡的功能，同一台设备提供不少6条链路负载均衡功能。支持多链路应用会话保持，支持多种链路检测方法，支持基于应用协议的智能选路，支持多种健康检查方式，支持硬件SSL卸载和加速功能，支持TCP协议优化，支持源NAT、目的NAT、一对一NAT、NAT地址池等NAT功能；支持包过滤功能。	台	1
5.	应用交付设备	设备具备6个千兆电口；硬件配置：内存4GB，存储介质128GB SSD；吞吐量2.1Gbps，并发会话数110万，四层每秒新建会话数9万，七层每秒新建会话数5万；	台	2
6.	企业级VPN网关	采用多核处理器硬件架构，吞吐量：30Gbps；并发连接数：15,000,000；每秒新建连接数：1,500,000. 配置1200个SSLVPN授权	台	1
7.	SSL VPN接入网关	4个千兆电口；SSLVPN加密流量100Mbps，SSLVPN并发用户数300（本次配置100并发用户授权），每秒新建用户数60，IPSec加密最大流量50Mbps，IPSec并发会话数3000，IPSec并发隧道数300，防火墙吞吐量150Mbps。	台	2
8.	万兆防火墙	产品形态：专业机架式产品；千兆光口24个，千兆电口8个，万兆光口2个，满配万兆多模光模块，扩展槽位2个，双交流电源冗余	台	4
9.	万兆入侵防御	产品形态：专业机架式产品；千兆光口24个，千兆电口8个，万兆光口2个，满配万兆多模光模块，扩展槽位2个，冗余电源	台	4
10.	路由交换网关	DPX8000-A5，以太网核心交换机，背板带宽：86.4Tbps，五槽位	台	2
11.	Web应用防护插卡	设备实配万兆光口4个，千兆光口36个，千兆电口12个，万兆多模光模块4个，双电源。性能指标：吞吐量12Gbps，并发连接数400万，每秒新建连接数15万，所有端口都开启了防护功能授权。	块	2
12.	漏洞扫描插卡	产品形态：千兆电口12个，千兆光口12个性能指标：最大IP扫描无限制，并发IP为70个，每IP最大线程8个，所有端口均开启扫描授权，实配512个IP地址及域名扫描授	块	2

序号	设备名称	主要性能、功能	单位	数量
		权, WEB 扫描授权功能。		
13.	服务器负载均衡	吞吐量: 30Gbps; 并发连接数: 12,000,000; 4层新建连接数: 550,000; 7层新建连接数: 1,200,000; 网络接口: 8个千兆电口, 8个千兆光口, 2个万兆光口, 2个扩展槽; 内存: 32GB; 硬盘: 500GB; 尺寸: 2U; 电源: 冗余电源。	套	2
14.	外联节点防火墙	采用多核处理器硬件架构, 吞吐量: 5Gbps; 并发连接数: 2,000,000; 每秒新建连接数: 150,000; 标配网口: 12个千兆电口, 1个扩展槽; 硬件BYPASS: 支持; 硬盘: 320GB; 电源: 单电源; 平均无故障时间(MTBF): 10年; 串口: 1个RJ45串口; USB: 2个USB口。	台	22
15.	万兆防火墙	网络层吞吐量 $\geq$ 16Gbps; 应用层吞吐量 $\geq$ 10Gbps; 并发连接数 $\geq$ 250万; $\geq$ 6个千兆电口, $\geq$ 4个千兆光口, $\geq$ 2个万兆光口, 配置两个万兆光模块, 双电源, 支持Bypass;	台	2
16.	边界防火墙	机架式设备, $\geq$ 6个千兆电口, 最大并发连接数 $\geq$ 150万, 每秒新建连接数 $\geq$ 15K, 吞吐量 $\geq$ 5Gbps, 支持BYPASS, 支持透明模式、路由模式和混合模式部署; 包过滤、应用状态检测防火墙, 支持IPsec VPN、SSL VPN	台	4
17.	上网行为管理 1	标准 1U 设备, 吞吐量 1.3Gbps, 并发会话数 1,220,000, 用户规模 6500, 具备 6 个千兆电口, 1 个 RJ45 串口, 硬盘 500GB, 支持 BYPASS;	台	1
18.	上网行为管理 2	标准 1U 设备, 吞吐量 1.2Gbps, 并发会话数 510,000, 用户规模 1400, 具备 6 个千兆电口, 1 个 RJ45 串口, 硬盘 500GB、支持 BYPASS; 设备支持以网关、网桥、旁路、多路桥模式部署;	台	1
(四) 防病毒及安全管理				
1.	终端检测响应系统	承担 300 点服务器操作系统客户端授权升级, 承担 450 点 PC 终端授权更新升级, 支持 Windows XP/VISTA/WIN7/WIN8/WIN10 和其他国产化终端, 可扩展其它操作系统平台和其它功能, 需每年升级服务。	套	1
(五) 数据安全审计及安全交换				
序号	设备名称	设备参数	单位	数量
1.	数据库审计引擎	天钥 CA2300ER, 配置上架专用设备、配置 1 千兆电口监听、4 个千兆电口、4 个 SFP 千兆插槽、1 个千兆管理口、双电源;	台	1

序号	设备名称	主要性能、功能	单位	数量
2.	数据库审计日志中心	天钥 CA2300SR, 配置上架专用设备、支持 4 个审计引擎、1 个 1000M 电口管理口、1 个 1000M 电口数据口、数据存储量 2T、支持 RAID5、双电源。含不少于 8 个被审计 DB 服务数, 千兆审计系统审计事件每秒入库速度至少在 20000 条/秒以上, 日处理审计事件数至少 1600 万条。	台	1
3.	单向隔离网闸	千兆电口 8 个, 千兆 SFP 插槽 4 个, USB 口 4 个, 内、外网有独立的管理接口, 内、外网具有独立的 HA 口。	台	2
4.	安全隔离网闸	X-GAP 7000-F, 内外网主机 $\geq 8$ 个 10/100/1000BASE-T 独立网络口(非管理口和 HA 口), $\geq 4$ 个千兆 SFP 接口, 单独提供独立的管理口, HA 双机热备口, 整机双向吞吐量 $\geq 2\text{Gbps}$ ; 支持文件交换、数据库同步、数据库访问、安全浏览、FTP 访问、邮件传输、定制访问、二次开发、流媒体传输等基本功能;	台	2
5.	物理隔离网闸(对接运政业务)	安全隔离与信息交换系统 V3 TopRules 60002U, 标配单电源; 内端机 6 个 10/100/1000Base-T 接口, 含 1 个 MAN 口和 1 个 HA 口; 外端机 6 个 10/100/1000Base-T 接口, 含 1 个 MAN 口和 1 个 HA 口; 吞吐量: 600Mbps。单向网闸(光闸), 标准配置含主动文件交换模块、被动文件交换模块、邮件传输模块、TCP 应用单向传输模块、UDP 应用单向传输模块。	台	1
6.	物理隔离网闸(对接网约车业务)	安全隔离与信息交换系统 TopRules 8000 内端机 4 个 10/100/1000Base-T 接口和 4 个 SFP 插槽, 1 个串口, 2 个 USB 口; 外端机 4 个 10/100/1000Base-T 接口和 4 个 SFP 插槽, 1 个串口, 2 个 USB 口。整机吞吐量 2000Mbps, 并发连接数 100000。支持并配置文件交换、数据库同步、数据库访问、安全浏览、FTP 访问、邮件传输、定制访问、二次开发、流媒体传输等基本功能; 支持并配置文件交换、数据库同步、数据库访问、安全浏览、FTP 访问、邮件传输、定制访问、二次开发、流媒体传输等基本功能;	台	1
(六) 其他网络安全设备(近海设备)				
1.	态势感知	SUR2000/V1.0	套	1
2.	漏洞扫描	NVS-6000, 8 个千兆电口; 支持 IP 地址段(256 个 IP 地址) 批量反查域名、内网穿透扫描;	套	1

序号	设备名称	主要性能、功能	单位	数量
		支持主机漏洞扫描、Web 漏洞扫描、弱密码扫描；		
3.	日志审计	TSOC-SA2100，通过监测及采集信息系统中的系统安全事件、用户访问行为、系统运行日志、系统运行状态等各类信息，经过规范化、过滤、归并和告警分析等处理后，实现对信息系统整体安全状况的全面管理。	套	1
4.	数据库审计	GE1500ER，支持审计 ORACLE、SQL Server、MY SQL、DB2、Sybase、Informix、Postgresql、Kingbase、Cache、Gbase、Dameng、Teradata、Oscar、Mongodb 等各类主流数据库系统审计	套	1
5.	堡垒机	OSM3600-，1U 机架式软硬一体设备，实现对运维操 telnet/ssh/ftp/sftp/RDP 的集中管理、访问控制、单点登录以及操作审计等功能。	套	1
6.	防火墙	四层吞吐量 16G，新建连接数 25 万。	台	2
7.		配置千兆以太网光接口 4；配置千兆以太网电接口 8，业务插槽 2，配置日志存储硬盘 600G，配置冗余电源。		
8.	入侵检测	1U 机架式。吞吐量 6G，新建连接数 9 万，并发连接数 300 万。业务口配置 8*GE 电口 +4*SFP 光口，配置本地硬盘存储日志信息和查看报表 600G，配置 2 个扩展插槽，配置冗余电源。配置入侵检测功能模块，能够检测各种应用层攻击，支持对 VLAN、IPv4、MPLS、GRE、IPv6、IPv4 over IPv6、IPv6 over IPv4 报文的入侵防护，支持 SSL 加密流量检测。	台	1
9.	通信外网负载均衡	1U 机架式设备，四层吞吐量 12G，新建连接数 20 万。配置千兆电口 8 个，千兆光口 4 个；配置冗余电源；配置 600G 硬盘。支持 VRRP、支持 Active/Active 和 Active/Passive 可识别应用层协议数量 6000 种。	台	2
10.	外联分支防火墙	四层吞吐量 600M，新建连接数 2.5 万；配置接口 4GE 电+2GE combo；业务插槽 2，支持日志存储硬盘，配置硬盘 600G；配置冗余电源。支持静态路由、策略路由、RIP、OSPF、BGP、ISIS 等路由协议。	台	20
(七) 数据视频汇聚安全设备				
1.	边界安全防火墙	网络层吞吐量 $\geq$ 4G，应用层吞吐量 $\geq$ 2G，防病毒吞吐量 $\geq$ 600M，IPS 吞吐量 $\geq$ 600M，全威胁吞吐量 $\geq$ 450M，并发连接数 $\geq$ 200 万，IPSec VPN 吞吐量 $\geq$ 270M；设备的硬件参数需满足规格 1U，内存大小 $\geq$ 4G，硬盘容量 $\geq$ 128GB SSD，	台	7

序号	设备名称	主要性能、功能	单位	数量
		接口：千兆电口 $\geq 8$ ，千兆光口 $\geq 2$ 。		
2.	深信服视频网闸	吞吐量 $\geq 5\text{Gbps}$ ，并发连接数 $\geq 50\text{W}$ 。吞吐量 $\geq 5\text{Gbps}$ ，最大并发连接数 $\geq 50$ 万。标配提供文件交换、数据库访问和同步、视频交换、组播代理、访问交换等功能模块。2U设备，“双主机+隔离卡”架构，单主机硬件信息 $\geq 6$ 电4光，内存 $\geq 4\text{GB}$ ，硬盘 $\geq 64\text{G SSD}$	台	1

#### 2.4.2 人员配置要求

(1) 项目驻场人员 1 名，应取得有效期内的 CISP、CISAW、CISP-PTE 等安全体系认证证书中的至少一项，且是服务商的正式员工，在本单位工作 1 年以上；

(2) 年度网络安全检查期间，现场驻守团队不少于 2 人（除本项目约定的驻场工程师外），协助完成网络安全自查报告；

(3) 重保期间现场值守团队不少于 2 人（除本项目约定的驻场工程师外），开展 7\*24 小时值守并每天形成日报告。

合同期内，设立驻场维保小组，当发生人员无法到岗时，需要有备用人员随时顶替。

人员工作时间满足《中华人民共和国劳动法》第三十六条要求。

#### 2.5 服务保障要求

(1) 供应商需要提供现场支持、远程技术支援和定期检查服务，确保采购方各系统的网络畅通。

(2) 在维护保养中，所更换的软件和硬件需具备稳定性、成熟性和兼容性，以不影响采购方的正常业务运作。

(3) 供应商及其员工必须对涉及的所有系统技术和数据信息严格保密。若出现因供应商原因导致的数据丢失、业务中断或其他损害采购方利益的情况，供应商应承担全部责任。

(4) 提供故障案例分析、文档管理和信息支持服务，以助采购方更好地理解和使用系统。

(5) 为关键业务数据提供备份服务，确保数据的安全性。

(6) 配合采购方每年完成至少一次的应用及数据安全应急演练，提高应对突发状况的能力。



(7)在特定时期如节假日、重大活动等，加强安全保障，进行安全检查，及时发现并修复潜在风险，确保信息化基础设施的正常运行。

(8)根据网络安全主管部门和第三方的建议，对存在的安全漏洞和风险进行及时整改，并提交整改报告。

(9)供应商及其驻场技术服务人员需签订“安全保密协议”，保证不会将服务中涉及的任何信息泄露或提供给第三方。

(10)供应商需承担与运维人员驻场服务相关的所有费用，包括但不限于场地租赁费、通勤费等。

(11)对于采购方提出的系统问题，供应商应在 20 分钟内响应，并在 4 小时内解决。在紧急情况下，供应商需提供实时响应，并在必要时提供备用机以确保业务的连续性。

(12)设备或零部件损坏，需调配同品牌同型号的备件对损坏设备或零部件进行免费更换。

(13)设备使用环境发生改变、设备现有性能无法正常运转、备份空间不足或者因设备故障维修成本过高等情况下，提供其他零散备品备件及辅材耗材等供应服务。

## 2.6 交付物

(1)制定《运维服务项目方案》并落实执行。

(2)编制日常巡检报告并向采购人汇报。

(3)编制季度设备整体运行情况评估分析报告并向采购人汇报。

(4)编制月度巡检报告并向采购人汇报。

(5)编制季度培训计划、方案等材料，完成相应技术培训。

(6)配合开展相关资产梳理，编制汇总相关信息。

(7)完成年度应急演练配合工作，编制相应证明材料。

(8)配合完成重大节假日、重点时期的安全保障工作并汇总存档日志、总结等材料。

工程量清单						
项目	任务描述	单位	数量	单价	合价	备注
一、常规运维工作						
(一) 日常检查						
1	设备日常巡查	次	1095			
(二) 预防性检查						
1	系统漏洞扫描	次	12			

2	系统优化补丁升级	次	随机			
3	设备整体运行情况评估分析	次	4			
4	技术培训	次	4			
5	网络配置变更操作	次	随机			
6	系统部署与维护	次	按需			
7	网络监控与性能优化	次	随机			
8	重要数据备份与恢复	次	按需			
(三) 应急检查						
1	设备应急检查及分析	次	按需			
二、非常规运维工作						
1	设备维修	项	1			设备可用率达到 98%
2	技术支持与服务	项	1			服务响应率达到 100%
3	设备升级与迁移	项	1			服务响应率达到 100%
4	应急保障服务	项	1			服务响应率达到 100%
三、费用合计						
			合计			

### 3. 商务条件

#### 3.1 服务期限

自签订合同之日起至 2024 年 9 月 30 日。

#### 3.2 服务团队要求

投标人须为本项目组建稳定的、专业的、独立的项目团队，团队成员需满足以下要求：

3.2.1 运营服务单位应确保运营团队人员稳定性，团队核心运营人员应具备运营服务工作统筹和技术把控能力，能够顺畅沟通和准确理解运营需求变化；

3.2.2 项目团队人员要严格遵守公司的各项规章制度和管理规定，具有很强的工作责任心和服务意识，配合采购人项目中工作需求，工作过程中严格遵循安全保密协议。

#### 3.3 付款方式

合同约定。

### 3.4 服务质量保证

投标人在服务过程中应保证项目实施方案完整，工作机制合理有效，项目组机构设置及职能划分明确，针对不同服务内容专门的项目质量管理保障，实施组织计划时间安排合理、项目特点突出、切实可行，能够保障交通运行预测研判报告编制的完整性、准确性和及时性。

### 3.5 服务成果验收

按照国家、省、市相关文件要求的有效规范和标准进行验收。

注：上述要求以及标注中：

带“★”条款为实质性条款，供应商必须按照磋商文件的要求做出实质性响应。

带“◆”标注的为可能实质性变动的技术、服务要求以及合同草案条款内容。

带“▲”标注的产品为政府强制采购产品，政府强制采购产品是指财政部、发展改革委最新一期发布“节能产品政府采购清单”中的政府强制采购节能产品。

带“※”标注的产品为供应商开启响应文件时需提供的样品，成交后成交供应商送至采购人指定地点封存。成交供应商提交的样品与响应文件不一致的，由成交供应商承担相关法律责任。

带“●”标注的产品为核心产品，系指在非单一产品采购项目中，采购人根据采购项目技术构成、产品价格比重等合理确定的产品。

## 第五章 评标办法

实行三轮报价法，第三轮报价为最终报价（其中第三轮报价需同时报出对应单价），第三轮报价最低的供应商为本项目中标人。参与谈判的承包商第一轮报价即为投标报价，在招标范围不变的情况下，以参与谈判的承包商第一轮报价中最低报价为谈判基准价，所有参与谈判的承包商第二轮报价不得高于该基准价，并且后一轮报价不得高于其前一轮报价，否则谈判小组有权据此确定为无效报价。若两家及以上承包商在第三轮报价中同为最低报价的，只给予同为最低报价的供应商追加报价机会（追加报价不受轮次限定，直至产生只有一家最低报价的供应商）。

# 响应文件

项目名称：

项目编号：

供应商全称（盖公章）：

二〇 年 月 日

## 目录

### 商务部分

- 1、报价一览表(见附件 1)；
- 2、响应报价明细表(见附件 2)；
- 3、报价函(见附件 3)；
- 4、在经营活动中没有重大违法记录的书面声明(见附件 4)；
- 5、法定代表人身份证明(见附件 5)；
- 6、法定代表人授权委托书(见附件 6)；
- 7、营业执照、资格资质证明材料复印件；
- 8、供应商同类项目实施情况一览表(见附件 7)；
- 9、项目实施人员(主要从业人员及其技术资格)一览表(见附件 8)；
- 10、中标服务费承诺书(见附件 9)；
- 11、政府采购诚信承诺书(见附件 10)；
- 12、招标文件其他规定或者供应商认为应介绍或者提交的资料，文件和说明。

### 技术部分（格式自拟）

附件 1:

### 报价一览表

项目名称:

项目内容	含税报价(元)	备注 (取费依据、收费标准等)
含税总报价(元)	大写:	
	小写:	

供应商名称(盖公章):

供应商法定代表人或者被授权代表:(签字)

时间: 年月日

附件 2:

### 分项报价明细表

项目名称:

序号	项目名称	服务说明	报价 (万元)	备注
1				
2				
3				
	.....			
服务项目费用合计		大写:		
		小写:		

1. 本表格为参考格式, 投标人可根据自身情况填报“费用明细”。

2. 投标人报价应考虑全面、取费合理、计算准确。

供应商名称(盖公章):

供应商法定代表人或者被授权代表(签字):

时间: 年月日

附件 3:

## 报价函

                     (采购人):

                     (供应商名称) 系中华人民共和国合法企业, 经营地址。

我            (姓名) 系                      (供应商名称) 的法定代表人, 我方愿意参加贵方组织的                      (项目名称)                      (编号为) 的报价, 为此, 我方就本次报价有关事项郑重声明如下:

- 1、我方已详细审查全部采购文件, 同意采购文件的各项要求。
- 2、我方向贵方提交的所有响应文件、资料都是准确的和真实的。
- 3、若中标, 我方将按照采购文件规定履行合同责任和义务。
- 4、我方不是采购人的附属机构; 在获知本项目采购信息后, 与采购人聘请的为此项目提供咨询服务的公司及其附属机构没有任何联系。
- 5、响应文件自开标日起有效期为 90 日历日。
6. 以上事项如有虚假或者隐瞒, 我方愿意承担一切后果。

供应商全称(公章):

法定代表人(签字或盖章):

日期:



附件 4:

### 在经营活动中没有重大违法记录的书面声明

一、我方在参加(项目名称)政府采购活动前 3 年内,在经营活动中:

1、没有重大违法记录(重大违法记录指供应商因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚)。

2、没有行贿犯罪记录(查询内容:①供应商名称、组织机构代码证或统一社会信用代码;②法定代表人、身份证号码;③项目负责人、身份证号码)。

二、我方在参加本项目活动前一段时间内具有良好的商业信誉和健全的财务会计制度、具有履行合同所必需的设备和专业技术能力、具有依法缴纳税收和社会保障资金的良好记录。

若以上声明不实,我方自愿承担一切法律后果。

供应商全称(公章):

日期:年月日

备注: 1. 采购文件未要求项目负责人的, 项目负责人一栏可删除。

附件 5:

## 法定代表人身份证明

供应商名称:

单位性质:

地址:

成立时间: 年 月 日

经营期限:

姓名: 性别: 年龄: 职务:

系 (供应商名称) 的法定代表人。

特此证明。

附: 法定代表人身份证复印件。

供应商: (公章)

年月日

附件 6:

## 法定代表人授权委托书

        (采购人):

我        (姓名)系        (供应商名称)法定代表人,现授权委托我公司的        (姓名、职务或者 职称)为我公司本次项目的授权代表,代表我方办理本次报价、签约等相关事宜,签署全部有关的文件、协议、合同并具有法律效力。

在我方未发出撤销授权委托书的书面通知以前,本授权委托书一直有效。被授权人 签署的所有文件(在授权书有效期内签署的)不因授权撤销而失效。

被授权代表无权转让委托权。特此授权。

本授权委托书于年月日签字生效,特此声明。

(附法人代表身份证以及被授权代表身份证复印件)

被授权代表姓名: 性别: 年龄:

单位: 部门: 职务:

供应商(公章):

法定代表人(签字或盖章):

日期: 年月日

附件 7:

### 供应商同类项目实施情况一览表

报价包：第 包

项目(包)名称：

采购单位名称	服务项目名称	单价	合同 金 额 (元)	附件页码	采购单位联系人 及 联系电话
				合同	
备注	供应商须提供同类项目合同复印件等相关证明材料。				

供应商名称(盖公章):

供应商法定代表人或者被授权代表: (签字)

时间: 年月日

附件 8:

### 项目实施人员(主要从业人员及其技术资格)一览表

报价包: 第 包

项目(包)名称:

姓名	职务	专业技 术资格	证书 编号	参加本单位工 作时间	劳动合 同编号

注: 在填写时, 如本表格不适合报价单位的实际情况, 可根据本表格式自行划表填写。

供应商名称(公章):

法定代表人或者被授权代表: (签字) 日期:

附件 9:

## 政府采购诚信承诺书

（采购人）：

我公司（供应商名称）已详细阅读了项目（项目编号：）采购文件，自愿参加本次报价，现就有关事项做出郑重承诺如下：

一、诚信报价，材料真实。我公司保证所提供的全部材料、报价内容均真实、合法、有效，保证不出借或者借用其他企业资质，不以他人名义报价，不弄虚作假；

二、遵纪守法，公平竞争。不与其他供应商相互串通、哄抬价格，不排挤其他供应商，不损害采购人的合法权益；不向谈判小组、采购人提供利益以牟取中标。

三、若中标后，将按照规定及时与采购人签订政府采购合同，不与采购人订立有悖于采购结果的合同或协议；严格履行政府采购合同，不降低合同约定的产品质量和服务，不得擅自变更、中止、终止合同，或者拒绝履行合同义务；

若有违反以上承诺内容的行为，我公司自愿接受取消报价资格、记入信用档案、媒体通报、1-3年内禁止参与政府采购等处罚；如已中标的，自动放弃中标资格，并承担全部法律责任；给采购人造成损失的，依法承担赔偿责任。

供应商名称(盖公章):

法定代表人(签章):

年月日

附件10:

响应文件包装袋密封件正面和封口格式

响应文件包装袋密封件正面格式

收件人:

项目名称:

项目编号:

响应文件（资格、资信等证明文件）

供应商名称:

供应商地址:

邮政编码:

20 年 月 日

加盖供应商公章（供应商法定代表人或者被授权代表签字或印章）

响应文件封口格式

请勿在20 年 月 日 时之前启封

加盖供应商公章（供应商法定代表人或者被授权代表签字或印章）

